UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,344	07/22/2003	Jeffrey S. Bardsley	5577-265	7591

20792 7590 08/11/2006

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/624,344	BARDSLEY ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/22/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims **1-23** have been examined.

Information Disclosure Statement PTO-1449

1. Information disclosure statements submitted by applicant dated 7/22/2003 was considered. Please see attachment PTO-1449.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 to 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Friedrichs et Al. (U.S. Patent Application Publication No. 2003/0084349 A1, filed August 9, 2002).

3.1. As per claim 1, Friedrichs is directed to a method of generating computer security threat management information (paragraph 8-10), comprising: receiving notification of a computer security threat (paragraph 40 to 44 or 20-30); generating a computer-actionable Threat Management Vector (TMV) from the notification that was received (as described in paragraph 39, the result of threat data collection and analysis are put in a report to be sent to viewing systems or a web server for storage. The reports are sent in form of a file, which is a computer actionable item, containing fields reflecting different information items), the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat (per paragraph 42, information stored in databases and included in the analysis and report includes demographic data. Per paragraph 35, the demographic data includes type of network and Operating System), a second computer-readable field that provides identification of a release level for the system type (per paragraph 42, the proprietary information of security devices are included in the databases for analysis and report, in addition to demographic information, which shows detailed specifications of systems involved in the security threat are completely collected in the databases, and reported as necessary) and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level (paragraph 45); and transmitting the TMV that is generated to a plurality of target systems for processing by the plurality of target systems (per paragraph 35, the generated reports are sent to different client systems).

3.2. As per claim 2, Friedrichs is directed to a method according to claim 1 wherein the generating comprises selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format (paragraphs 40-45, and paragraph 46 showing all mentioned databases could be combined to one database).

3.3. As per claim 3, Friedrichs is directed to a method according to claim 1 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level (paragraph 35 and 42).

3.4. As per claim 4, Friedrichs is directed to a method according to claim 1 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation (paragraph 45, detailing how a countermeasure can be implemented and installed).

3.5. As per claim 5, Friedrichs is directed to a method according to claim 1 wherein at least one of the identifications comprises a pointer (pointers are broadly used in databases to identify data).

3.6. As per claim 6, Friedrichs is directed to a method according to claim 1 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security

threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level (per paragraph 22, the Security Device 110 gathers details of elements participating in the threat. The details include ports, which is a subsystem if a network element. In addition, Hunter server 140 gathers further details such as IP address of system. As described in response to claim 1, the version level of subsystems are also collected and reported as the comprehensive data about systems participating in the threat are recorded and reported).

3.7. As per claim 7, Friedrichs is directed to a method according to claim 6 wherein the subsystem type comprises an application program type (paragraph 35).

3.8. As per claim 8, Friedrichs is directed to a method according to claim 1 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat (per paragraph 43, Vendor signature databases contain a listing of all known security event types for a particular vendor, and therefore identifies the threats).

3.9. Limitations of claims 9 and 10 are substantially the same as claim 1 above.

3.10. As per claim 11, Friedrichs is directed to a system according to claim 9 further comprising a common semantics database that lists system types, release levels and possible countermeasures in a computer-readable format (Fig. 4 and associated text), wherein the TMV generator is responsive to the common semantics database to generate the TMV based upon user selection of a system type, release level and possible countermeasures from the common semantics database for the computer security threat (generation of a report based on user defined parameters was a well-known feature of database management systems at the time of invention).

3.11. Claims 12 to 23 are substantially the same as claims 1-8 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132

KAMBIZ ZAND
PRIMARY EXAMINER